UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF PENNSYLVANIA

ANTHONY COLLINS, individually and on behalf of all others similarly situated, Plaintiff, v. **IMAGINE360, LLC** Defendant.	Case No. **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Anthony Collins, individually and on behalf of all similarly situated persons, alleges the following against Imagine360, LLC ("Imagine360" or "Defendant") based upon personal knowledge with respect to himself and on information and belief derived from, among other things, investigation by his counsel and review of public documents as to all other matters:

I. INTRODUCTION

1. Plaintiff brings this class action against Defendant for its failure to properly secure and safeguard his and other similarly situated individuals' (defined herein as "Class Members") personally identifiable information ("PII") and protected health information ("PHI"), including names, addresses, medical billing and insurance information, certain medical information such as diagnoses and medication, and demographic information such as dates of birth and Social Security numbers (the "Private Information"), from unauthorized disclosure to cybercriminals.

2. Defendant Imagine360 is a healthcare revenue cycle company located in Wayne, Pennsylvania that maintains the PII and PHI of employees of its clients, including Plaintiff's employer, Lapham-Hickey Steel Corp. ("Lapham").

3. Plaintiff brings this class action lawsuit to address Defendant's collective inadequate safeguarding and supervision of Class Members' Private Information that they collected and maintained, and its failure to adequately supervise its business associates, vendors, and/or suppliers and timely detect the Data Breach.

4. On or about January 30, 2023 or earlier, an unauthorized third party or person accessed and downloaded Plaintiff's and Class Members' Private Information. Defendant has independent, non-delegable duties to its clients' employees to safeguard their PHI and PII and is responsible for the wrongful disclosure of Plaintiff's and Class Members' Private Information.

5. On February 1, 2023, cybersecurity expert Brian Krebs reported that Fortra, LLC ("Fortra") disclosed to its customers, including Citrix Systems ("Citrix") (another one of Defendant's business associates) of a "remote code injection exploit" affecting GoAnywhere MFT, Fortra's widely used file transfer application. Hackers used "remote code injection exploits" to remotely execute malicious code on their targets' computer systems.

6. On or around February 10, 2023, the Russia-linked ransomware group Clop claimed to be responsible for attacks on GoAnywhere MFT, and to have stolen data exposed by the software from over 130 organizations over the course of the preceding ten days, including Imagine360.

7. On February 22, 2023, the U.S. Department of Health and Human Services' ("HHS") Health Sector Cybersecurity Coordination Center issued a "Sector Alert" emphasizing that Clop's claim referenced its ability to target health care systems.

8. On June 9, 2023, in a Notice of Security Incident letter (the "Notice") sent to Plaintiff and Class Members, Defendant confirmed that the PII and PHI of certain of its clients' employees, including that of Plaintiff, were exposed by the threat actor (the "Data Breach"). It is

estimated that almost half a million individuals whose Private Information was in the possession and care of Imagine360 were impacted by the Data Breach.[1]

9. Upon information and belief, Defendant knew of the vulnerability in its internal file transfer system and/or of its business associates' lax data security practices, procedures, and protocols on or before January 29, 2023.[2] As such, Defendant could have prevented the Data Breach. However, Defendant's business associates had to inform Defendant of the Data Breach (despite Defendant's knowledge of the vulnerability and/or of its business associates' lax data security practices, procedures, and protocols) after the compromise and exfiltration of Plaintiff's and Class Members' Private Information had already occurred.

10. Defendant also could have prevented this theft had it limited the information it shared with its business associates, particularly Citrix and Fortra, and employed reasonable supervisory measures to ensure that adequate data security practices, procedures, and protocols were being implemented and maintained by said business associates in order to secure and protect the Private Information.

11. Defendant failed to comply with industry standards to protect highly sensitive PII and PHI and failed to provide adequate notice to Plaintiff and other Class Members that their PII and PHI had been compromised. Plaintiff seeks, among other things, orders requiring Defendant to fully and accurately disclose the nature of the information that has been compromised and to adopt sufficient security practices and safeguards to prevent incidents like the Data Breach in the future.

---

[1] *See* https://www.prnewswire.com/news-releases/nearly-a-half-million-social-security-numbers-leaked-following-data-breach-at-intellihartx-llc-301848518.html (last visited on June 20, 2023).

[2] *See* https://www.techtarget.com/searchsecurity/news/365535543/Fortra-completes-GoAnywhere-MFT-investigation (last visited on May 3, 2023).

12. Plaintiff and Class Members would not have allowed their Private Information to be entrusted to Defendant if they had known that Defendant would breach its promises and agreements by (a) failing to ensure that its vendors used adequate security measures, and/or (b) providing individuals' highly sensitive PII and PHI to business associates that utilized inadequate security measures.

13. Armed with the Private Information accessed in the Data Breach, data thieves can and will commit a variety of crimes against Plaintiff and Class Members, including, *e.g.*, opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' names to obtain medical services in Class Members' names, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

14. There has been no assurance offered by Defendant that all personal data or copies of data have been recovered or destroyed, or that Defendant have adequately enhanced its data security practices sufficient to avoid a similar breach of its network in the future.

15. Therefore, Plaintiff and Class Members have suffered and are at an imminent, immediate, and continuing increased risk of suffering, ascertainable losses in the form of harm from identity theft and other fraudulent misuse of their Private Information, including out-of-pocket expenses incurred to remedy or mitigate the effects of the Data Breach, and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach.

16. Plaintiff brings this class action lawsuit to address Defendant's inadequate safeguarding and supervision of Class Members' Private Information that it collected and maintained. The potential for improper disclosure and theft of Plaintiff's and Class Members'

Private Information was a known risk to Defendant, thus Defendant was on notice that failing to take necessary steps to secure the Private Information left it vulnerable to an attack.

17. Upon information and belief, Defendant failed to properly supervise its business associates and monitor the computer network and systems that housed the Private Information. Had Defendant provided adequate supervision over its agents, vendors, and/or suppliers, it could have prevented the Data Breach.

18. Plaintiff's and Class Members' identities are now at risk because of Defendant's negligent conduct as the Private Information that Defendant collected and maintained and failed to monitor is now in the hands of data thieves and other unauthorized third parties.

19. Plaintiff seeks to remedy these harms on behalf of himself and all similarly situated individuals whose Private Information was accessed and/or compromised during the Data Breach.

II. PARTIES

20. Plaintiff Anthony Collins is, and at all times mentioned herein was, an individual citizen of the State of Illinois.

21. Defendant Imagine360, LLC is headquartered and maintains its principal place of business at 1550 Liberty Ridge Dr. #330, Wayne, Pennsylvania in Delaware County.

III. JURISDICTION AND VENUE

22. This Court has original jurisdiction under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2), because this is a class action involving more than 100 putative class members and the amount in controversy exceeds $5,000,000, exclusive of interest and costs. Minimal diversity is established because Plaintiff (and many members of the Class) are citizens of states different than Imagine360.

23. This Court has general personal jurisdiction over Imagine360 because Imagine360's principal place of business and headquarters are in this District. Imagine360 also regularly conducts substantial business in this District.

24. Venue is proper in this District under 28 U.S.C. §§ 1391(a)(2), 1391(b)(2), and 1391(c)(2) because a substantial part of the events giving rise to the claims emanated from activities within this District, and Imagine360 conducts substantial business in this District.

IV. FACTUAL ALLEGATIONS

A. Defendant's Business and Collection of Plaintiff's and Class Members' Private Information

25. Imagine360 provides self-funded health insurance plan services to employers within a number of different industries, including auto dealing, convenience stores, construction, manufacturing, nonprofits, marine services, restaurants, senior living, trucking and transportation, technology, and professional services.[3]

26. According to its own website, Imagine360 was founded on the "powerful idea" that "[h]ealth plans can do better[,]" and "[e]mployees should get the high-quality care they need at a fair price."[4]

27. As a condition of receiving these services, Defendant requires that its employer clients, including Plaintiff's employer, turn over highly sensitive employee personal and health information.

28. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Private Information, Defendant assumed legal and equitable duties owed to them and

[3] *See* https://www.imagine360.com/industries/ (last visited on July 6, 2023).
[4] *See* https://www.imagine360.com/about/ (last visited on July 6, 2023).

knew or should have known that it was responsible for protecting Plaintiff's and Class Members' Private Information from unauthorized disclosure and exfiltration.

29. Plaintiff and Class Members relied on Defendant to keep their Private Information confidential and securely maintained and to only make authorized disclosures of this Information, which Defendant ultimately failed to do.

B. The Data Breach

30. Fortra and Citrix were Defendant's "business associates." Nevertheless, on February 1, 2023, cybersecurity expert Brian Krebs reported that Fortra disclosed to its customers a "remote code injection exploit" affecting GoAnywhere MFT, Fortra's widely used file transfer application. Hackers used "remote code injection exploits" to remotely execute malicious code on their targets' computer systems.

31. On or around February 10, 2023, the Russia-linked ransomware group, Clop, claimed to be responsible for attacks on GoAnywhere MFT and to have stolen data exposed by the software from over 130 organizations over the course of the preceding ten days.

32. On June 30, 2023, Imagine360 reported through its Notice to the Maine Attorney General's office and by direct letter notice to Plaintiff and Class Members that it was one of the entities impacted, and that the PII and PHI of certain employees of its clients, including Lapham – Plaintiff's employer – were exposed in the attack.

33. Through the Data Breach, the unauthorized cybercriminals accessed a cache of highly sensitive Private Information, including sensitive medical information and health insurance information.

34. Defendant delivered its Notice to Plaintiff and Class Members on or around June 30, several months following the Data Breach, alerting them that their highly sensitive Private Information had been exposed.

35. Defendant had obligations created by contract, industry standards, common law, federal and state regulations, and representations made to Plaintiff and Class Members to keep Plaintiff's and Class Members' Private Information confidential and to protect it from unauthorized access and disclosure.

36. Plaintiff and Class Members permitted their employers to provide their Private Information to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such Information confidential and secure from unauthorized access. In Plaintiff's case, his Private Information was provided to Defendant in order to process claims associated with his health insurance plan obtained through his employer.

37. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks in recent years.

38. Defendant knew or should have known that its electronic records would be targeted by cybercriminals, particularly in light of one of its associates, Citrix's, recent history of data breaches.[5]

C. The Healthcare Sector is Particularly Susceptible to Data Breaches

39. Defendant was on notice that companies in the healthcare industry, including its business associate, Citrix, are susceptible targets for data breaches.

[5] *See* https://krebsonsecurity.com/2020/02/hackers-were-inside-citrix-for-five-months/; *see also* https://www.cybersecuritydive.com/news/citrix-vulnerability-exploited-ransomware/640389/ (last visited on July 6, 2023).

40. Defendant was also on notice that the FBI has been concerned about data security in the healthcare industry. In August 2014, after a cyberattack on Community Health Systems, Inc., the FBI warned companies within the healthcare industry that hackers were targeting them. The warning stated that "[t]he FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining the Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PII)."[6]

41. The American Medical Association ("AMA") has also warned healthcare companies about the importance of protecting confidential medical information:

> Cybersecurity is not just a technical issue; it's a patient safety issue. AMA research has revealed that 83% of physicians work in a practice that has experienced some kind of cyberattack. Unfortunately, practices are learning that cyberattacks not only threaten the privacy and security of patients' health and financial information, but also patient access to care.[7]

42. The healthcare sector reported the second largest number of data breaches among all measured sectors in 2018, with the highest rate of exposure per breach.[8] In 2022, the largest growth in data compromises occurred in the healthcare sector.[9]

---

[6] Jim Finkle, *FBI Warns Healthcare Firms that they are Targeted by Hackers*, Reuters (Aug. 2014), *available at* https://www.reuters.com/article/us-cybersecurity-healthcare-fbi/fbi-warns-healthcare-firms-they-are-targeted-by-hackers-idUSKBN0GK24U20140820 (last visited on April 28, 2023).

[7] Andis Robeznieks, *Cybersecurity: Ransomware attacks shut down clinics, hospitals*, Am. Med. Ass'n. (Oct. 4, 2019), *available at*: https://www.ama-assn.org/practice-management/sustainability/cybersecurity-ransomware-attacks-shut-down-clinics-hospitals (last visited on April 28, 2023).

[8] Identity Theft Resource Center, *2018 End-of-Year Data Breach Report, available at*: https://www.idtheftcenter.org/2018-data-breaches/ (last visited on April 28, 2023).

[9] Identity Theft Resource Center, *2022 End-of-Yeare Data Breach Report, available at*: https://www.idtheftcenter.org/wp-content/uploads/2023/01/ITRC_2022-Data-Breach-Report_Final-1.pdf (last visited on April 28, 2023).

43. Indeed, when compromised, healthcare related data is among the most sensitive and personally consequential. A report focusing on healthcare breaches found that the "average total cost to resolve an identity theft-related incident … came to about $20,000," and that the victims were often forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[10]

44. Almost 50 percent of the victims lost their healthcare coverage as a result of the incident, while nearly 30 percent said their insurance premiums went up after the event. Forty percent of the customers were never able to resolve their identity theft at all. Data breaches and identity theft have a crippling effect on individuals and detrimentally impact the economy as a whole.[11]

45. Healthcare related breaches have continued to rapidly increase because electronic patient data is seen as a valuable asset. "Hospitals have emerged as a primary target because they sit on a gold mine of sensitive personally identifiable information for thousands of patients at any given time. From social security and insurance policies, to next of kin and credit cards, no other organization, including credit bureaus, have so much monetizable information stored in their data centers."[12]

46. Defendant knew, or should have known, the importance of safeguarding its clients' employees' Private Information, including PHI, entrusted to it, and of the foreseeable

[10] Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (March 3, 2010), *available at:* https://www.cnet.com/news/privacy/study-medical-identity-theft-is-costly-for-victims/ (last visited on April 28, 2023).

[11] *Id*.

[12] Inside Digital Health, *How to Safeguard Hospital Data from Email Spoofing Attacks*, April 4, 2019, *available at*: https://www.chiefhealthcareexecutive.com/view/how-to-safeguard-hospital-data-from-email-spoofing-attacks (last visited on April 28, 2023).

consequences if such data were to be disclosed. These consequences include the significant costs that would be imposed on affected individuals as a result of a data breach. Defendant failed, however, to take adequate cybersecurity measures to prevent the Data Breach from occurring.

D. Defendant Failed to Comply with HIPAA

47. Title II of HIPAA contains what are known as the Administration Simplification provisions. *See* 42 U.S.C. §§ 1301, *et seq*. These provisions require that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling PHI similar to the data Defendant left unguarded and vulnerable to attack. The HHS has subsequently promulgated five rules under authority of the Administrative Simplification provisions of HIPAA.

48. The Data Breach resulted from a combination of insufficiencies that indicate Defendant failed to comply with safeguards mandated by HIPAA regulations and industry standards. First, it can be inferred from the Data Breach that Defendant either failed to implement, or inadequately implemented, information security policies or procedures to protect Plaintiff's and Class Members' PHI.

49. Plaintiff's and Class Members' Private Information compromised in the Data Breach included "protected health information" as defined by CFR § 160.103.

50. 45 CFR § 164.402 defines "breach" as "the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part which compromises the security or privacy of the protected health information."

51. 45 CFR § 164.402 defines "unsecured protected health information" as "protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the [HHS] Secretary[.]"

52. Plaintiff's and Class Members' Private Information included "unsecured protected health information" as defined by 45 CFR § 164.402.

53. Plaintiff's and Class Members' unsecured PHI was acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E, as a result of the Data Breach.

54. Based upon Imagine360's Notice to Plaintiff and Class Members, Defendant reasonably believes that Plaintiff's and Class Members' unsecured PHI has been acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E, as a result of the Data Breach.

55. Plaintiff's and Class Members' unsecured PHI that was acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E as a result of the Data Breach was not rendered unusable, unreadable, or indecipherable to unauthorized persons.

56. Defendant reasonably believes that Plaintiff's and Class Members' unsecured PHI that was acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E as a result of the Data Breach was not rendered unusable, unreadable, or indecipherable to unauthorized persons.

57. Plaintiff's and Class Members' unsecured PHI that was acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E as a result of the Data Breach, and which was not rendered unusable, unreadable, or indecipherable to unauthorized persons, was viewed by unauthorized persons.

58. Plaintiff's and Class Members' unsecured PHI was viewed by unauthorized persons in a manner not permitted under 45 CFR, Subpart E as a result of the Data Breach.

59. Defendant reasonably believes that Plaintiff's and Class Members' unsecured PHI was viewed by unauthorized persons in a manner not permitted under 45 CFR, Subpart E as a result of the Data Breach.

60. It is reasonable to infer that Plaintiff's and Class Members' unsecured PHI that was acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E as a result of the Data Breach, and which was not rendered unusable, unreadable, or indecipherable to unauthorized persons, was viewed by unauthorized persons.

61. It should be rebuttably presumed that unsecured PHI acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E, and which was not rendered unusable, unreadable, or indecipherable to unauthorized persons, was viewed by unauthorized persons.

62. After receiving notice that they were victims of the Data Breach (which required the filing of a data breach report in accordance with 45 CFR § 164.408(a)), it is reasonable for recipients of that notice, including Plaintiff and Class Members in this case, to believe that future harm (including medical identity theft) is real and imminent, and to take steps necessary to mitigate that risk of future harm.

63. Defendant's security failures also include, but are not limited to:

a. Failing to maintain adequate data security systems, practices, and protocols to prevent data loss;

b. Failing to mitigate the risks of a data breach and loss of data;

c. Failing to ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity *or business associate* creates, receives, maintains, or transmits" and "protect against any reasonably anticipated

threats or hazards to the security or integrity of such information," in violation of 45 C.F.R. § 164.306 (emphasis added);

d. Failing to ensure the confidentiality and integrity of electronic protected health information Defendant creates, receives, maintains, and transmits in violation of 45 CFR 164.306(a)(1);

e. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 CFR 164.308(a)(1);

f. Failing to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity, in violation of 45 CFR 164.308(a)(6)(ii);

g. Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic protected health information, in violation of 45 CFR 164.306(a)(2);

h. Failing to protect against any reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information, in violation of 45 CFR 164.306(a)(3); and

i. Impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons, in violation of 45 CFR 164.502, *et seq.*

64. Because Defendant failed to comply with HIPAA, while monetary relief may cure some of Plaintiff's and Class Members' injuries, injunctive relief is also necessary to ensure Defendant's approach to information security, especially as such approach relates to the supervision of its business associates, vendors, and/or suppliers, is adequate and appropriate going

forward. Defendant still maintains the PHI and other highly sensitive PII of its clients' current and former employees. Without the supervision of the Court through injunctive relief, Plaintiff's and Class Members' Private Information remains at risk of subsequent data breaches.

E. Defendant Failed to Comply with FTC Guidelines

65. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making. Indeed, the FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

66. In October 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cybersecurity guidelines for businesses. The guidelines note that businesses should ensure the protection of the personal customer information that they collect, properly dispose of personal information that is no longer needed, encrypt information stored on computer networks, understand their network's vulnerabilities, and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs, monitor all incoming traffic for activity indicating someone is attempting to hack into the system, watch for large amounts of data being transmitted from the system, and have a response plan ready in the event of a breach.

67. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction, limit access to sensitive data, require complex passwords

to be used on networks, use industry-tested methods for security, monitor the network for suspicious activity, and verify that third-party service providers have implemented reasonable security measures.

68. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data by treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by the FTCA. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

69. As evidenced by the Data Breach, Defendant failed to properly implement basic data security practices. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiff's and Class Members' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA.

70. Defendant was at all times fully aware of its obligations to protect the Private Information of its clients' employees yet failed to comply with such obligations. Defendant was also aware of the significant repercussions that would result from its failure to do so.

F. Defendant Breached Its Duty to Safeguard Plaintiff's and Class Members' Private Information

71. In addition to its obligations under federal and state laws, Defendant owed a duty to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendant owed a duty to Plaintiff and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its computer systems, networks, and protocols (and

those of its business associates, vendors, and/or suppliers) adequately protected the Private Information of Class Members.

72. Defendant breached its obligations to Plaintiff and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and data (and those of its business associates, vendors, and/or suppliers). Defendant's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to adequately protect Class Members' Private Information;

b. Failing to sufficiently train and/or monitor its business associates, vendors, and/or suppliers regarding the proper handling of its clients' employees' Private Information;

c. Failing to fully comply with FTC guidelines for cybersecurity in violation of the FTCA;

d. Failing to adhere to HIPAA and industry standards for cybersecurity, as discussed above; and

e. Otherwise breaching its duties and obligations to protect Plaintiff's and Class Members' Private Information.

73. Had Defendant remedied the deficiencies in its information storage and security practices, procedures, and protocols, followed industry guidelines, and adopted data security monitoring, supervision, and other measures recommended by experts in the field, it could have prevented the theft of Plaintiff's and Class Members' confidential Private Information.

74. Accordingly, Plaintiff's and Class Members' lives have been severely disrupted. What's more, they have been harmed as a result of the Data Breach and now face an increased risk of future harm that includes, but is not limited to, medical fraud and identity theft.

G. Defendant Should Have Known that Cybercriminals Target PII and PHI to Carry Out Fraud and Identity Theft

75. The FTC hosted a workshop to discuss "informational injuries," which are injuries that consumers like Plaintiff and Class Members suffer from privacy and security incidents such as data breaches or unauthorized disclosure of data.[13] Exposure of highly sensitive personal information that a consumer wishes to keep private may cause harm to the consumer, such as the ability to obtain or keep employment. Consumers' loss of trust in e-commerce also deprives them of the benefits provided by the full range of goods and services available which can have negative impacts on daily life.

76. Any victim of a data breach is exposed to serious ramifications regardless of the nature of the data that was breached. Indeed, the reason why criminals steal information is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims or to take over victims' identities in order to engage in illegal financial transactions under the victims' names.

77. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity or to otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired

[13] *FTC Information Injury Workshop, BE and BCP Staff Perspective,* Federal Trade Commission, (October 2018), *available at* https://www.ftc.gov/system/files/documents/reports/ftc-informational-injury-workshop-be-bcp-staff-perspective/informational_injury_workshop_staff_report_-_oct_2018_0.pdf (last visited on April 28, 2023).

information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

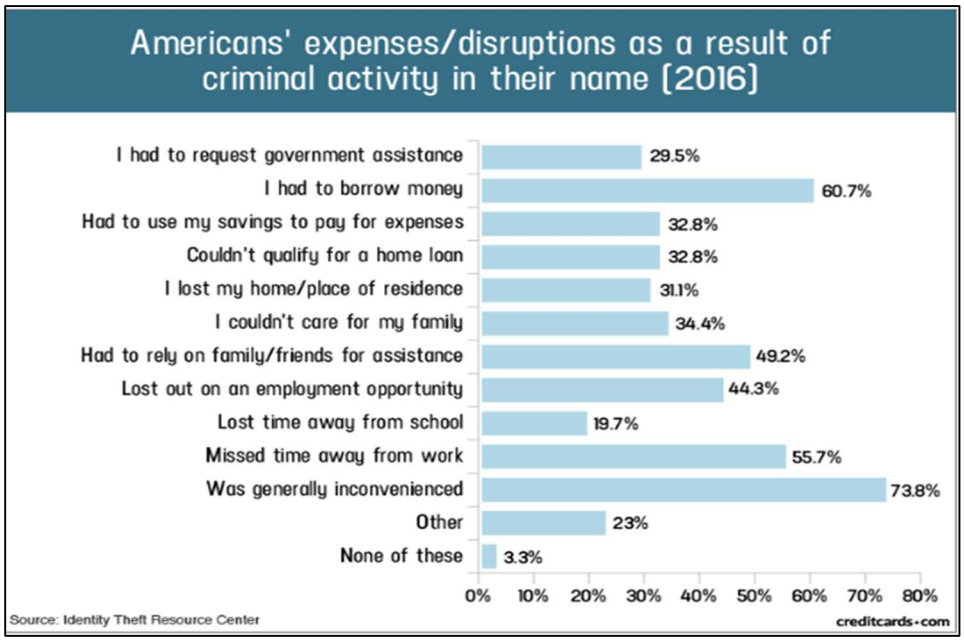
78. In fact, as technology advances, computer programs may scan the Internet with a wider scope to create a mosaic of information that may be used to link compromised information to an individual in ways that were not previously possible. This is known as the "mosaic effect." Names and dates of birth, combined with contact information like telephone numbers and email addresses, are very valuable to hackers and identity thieves as it allows them to access users' other accounts.

79. Thus, even if certain information was not purportedly involved in the Data Breach, the unauthorized parties could use Plaintiff's and Class Members' Private Information to access accounts, including, but not limited to, email accounts and financial accounts, to engage in a wide variety of fraudulent activity against Plaintiff and Class Members.

80. For these reasons, the FTC recommends that identity theft victims take several time-consuming steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert on their account (and an extended fraud alert that lasts for 7 years if someone steals the victim's identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a freeze on their credit, and correcting their credit reports.[14] However, these steps do not guarantee protection from identity theft but can only mitigate identity theft's long-lasting negative impacts.

[14] *See IdentityTheft.gov,* Federal Trade Commission, *available at* https://www.identitytheft.gov/Steps (last visited April 28, 2023).

81. In fact, a study by the Identity Theft Resource Center[15] shows the multitude of harms caused by fraudulent use of PII:



82. PHI is also especially valuable to identity thieves. As the FTC recognizes, identity thieves can use PHI to commit an array of crimes, including identity theft and medical and financial fraud.[16]

83. Indeed, a robust cyber black market exists in which criminals openly post stolen PHI on multiple underground Internet websites, commonly referred to as the dark web.

[15] Steele, Jason, *Credit Card and ID Theft Statistics*, CreditCards.com (October 23, 2017), *available at* https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276/ (last visited on April 28, 2023).

[16] Federal Trade Commission, *Warning Signs of Identity Theft, available at*: https://consumer.ftc.gov/articles/what-know-about-identity-theft (last visited on April 28, 2023).

84. While credit card information and associated PII can sell for as little as $1-$2 on the black market, protected health information can sell for as much as $363 according to the Infosec Institute.[17]

85. PHI is particularly valuable because criminals can use it to target victims with frauds and scams that take advantage of the victim's medical conditions or victim settlements. It can be used to create fake insurance claims, allowing for the purchase and resale of medical equipment, or gain access to prescriptions for illegal use or resale.

86. Medical identity theft can result in inaccuracies in medical records and costly false claims. It can also have life-threatening consequences. If a victim's health information is mixed with other records, it can lead to misdiagnosis or mistreatment. "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy Forum. "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."[18]

87. The ramifications of Defendant's failure to keep its clients' employees' Private Information secure are long-lasting and severe. Once it is stolen, fraudulent use of such and damage to victims may continue for years.

88. Here, not only was sensitive medical information compromised, but Social Security numbers may have been compromised too. The value of both PII and PHI is axiomatic. The value of "big data" in corporate America is astronomical. The fact that identity thieves attempt to steal

[17] Center for Internet Security, *Data Breaches: In the Healthcare Sector, available at*: https://www.cisecurity.org/insights/blog/data-breaches-in-the-healthcare-sector (last visited on April 28, 2023).

[18] Michael Ollove, "The Rise of Medical Identity Theft in Healthcare," Kaiser Health News, Feb. 7, 2014, *available at*: https://kffhealthnews.org/news/rise-of-indentity-theft/ (last visited on April 28, 2023).

identities notwithstanding possible heavy prison sentences illustrates beyond a doubt that the Private Information compromised here has considerable market value.

89. It must also be noted that there may be a substantial time lag between when harm occurs and when it is discovered, and also between when PII and/or PHI is stolen and when it is misused. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:[19]

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

90. PII and PHI are such valuable commodities to identity thieves that once the information has been compromised, criminals often trade the information on the dark web for years.

91. As a result, Plaintiff and Class Members are at an increased risk of fraud and identity theft, including medical identity theft, for many years into the future. Thus, Plaintiff and Class Members have no choice but to vigilantly monitor their accounts for many years to come.

H. Plaintiff's and Class Members' Damages

92. Plaintiff and Class Members have been damaged by the compromise of their Private Information in the Data Breach.

[19] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO (June 2007), *available at* https://www.gao.gov/assets/270/262904.html (last visited April 28, 2023).

93. Plaintiff and Class Members entrusted their Private Information to Defendant in order to receive Defendant's services. Specifically, Plaintiff Collins entrusted his Private Information to Defendant when he became an employee of Lapham.

94. Plaintiff's and Class Members' Private Information was subsequently compromised as a direct and proximate result of the Data Breach, which Data Breach resulted from Defendant's inadequate data security practices, procedures, and protocols, as discussed herein.

95. As a direct and proximate result of Defendant's actions and omissions, Plaintiff and Class Members have been harmed and are at an imminent, immediate, and continuing increased risk of harm, including but not limited to, having medical services billed in their names, along with other targeted forms of medical identity theft.

96. Further, as a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been forced to spend time dealing with the effects of the Data Breach. Specifically, Plaintiff and Class Members have also been forced to take the time and effort to mitigate the actual and potential impact of the data breach on their everyday lives, including placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, and/or closely reviewing and monitoring bank accounts, credit reports, and explanations of benefits for unauthorized activity for years to come.

97. Plaintiff and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

98. Plaintiff and Class Members also suffered a loss of value of their Private Information when it was acquired by cyber criminals in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in related cases. Indeed, an active and robust

legitimate marketplace for Private Information also exists. In 2019, the data brokering industry was worth roughly $200 billion.[20] In fact, the data marketplace is so sophisticated that consumers can sell their non-public information directly to a data broker who in turn aggregates the information and provides it to other companies.[21] Consumers who agree to provide their web browsing history to the Nielsen Corporation can in turn receive up to $50 a year.[22]

99. As a result of the Data Breach, Plaintiff's and Class Members' Private Information, which has an inherent market value in both legitimate and illegal markets, has been harmed and diminished due to its acquisition by cybercriminals. This transfer of valuable information happened with no consideration paid to Plaintiff or Class Members for their property, resulting in an economic loss. Moreover, the Private Information is apparently readily available to others, and the rarity of the Private Information has been destroyed because it is no longer only held by Plaintiff and the Class Members, and because that data no longer necessarily correlates only with activities undertaken by Plaintiff and the Class Members, thereby causing additional loss of value.

100. Plaintiff and Class Members also face a substantial risk of being targeted in future phishing, data intrusion, and other illegal schemes through the misuse of their Private Information, since potential fraudsters will likely use such Private Information to carry out such targeted schemes against Plaintiff and Class Members.

101. The Private Information maintained by and stolen from Defendant's systems, combined with publicly available information, allows nefarious actors to assemble a detailed mosaic of Plaintiff and Class Members, which can also be used to carry out targeted medical fraud and/or identity theft against them.

---

[20] See Data Coup, https://datacoup.com/ (last visited on May 30, 2023).
[21] *What is digi.me?, DIGI.ME,* https://digi.me/what-is-digime/ (last visited on May 30, 2023).
[22] *Frequently Asked Questions,* Nielsen Computer & Mobile Panel, https://computermobilepanel.nielsen.com/ui/US/en/faqen.html (last visited May 30, 2023).

102. Finally, Plaintiff and Class Members have suffered or will suffer actual injury as a direct and proximate result of the Data Breach in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach. These losses include, but are not limited to, the following, monitoring and reviewing explanations of benefits for fraudulent medical charges for years to come, as well as placing "freezes" and "alerts" with credit reporting agencies.

103. Moreover, Plaintiff and Class Members have an interest in ensuring that their Private Information, which is believed to still be in the possession of Defendant and its business associates, vendors, and/or suppliers, is protected from future breaches by the implementation of more adequate data security measures and safeguards.

104. As a direct and proximate result of Defendant's actions and inactions, Plaintiff and Class Members have suffered a loss of privacy and have suffered cognizable harm, including an imminent and substantial future risk of harm, in the forms set forth above.

V. CLASS ACTION ALLEGATIONS

105. Plaintiff brings this action individually and on behalf of all other persons similarly situated, pursuant to Fed. R. Civ. P. 23.

106. Specifically, Plaintiff proposes the following Nationwide Class (also referred to herein as the "Class"), subject to amendment as appropriate:

> **Nationwide Class**
> **All individuals in the United States who were impacted by the Data Breach, including all to whom Defendant sent a notice of the Data Breach**.

107. Excluded from the Class are Defendant and its parents or subsidiaries, any entities in which they have a controlling interest, as well as its officers, directors, affiliates, legal

representatives, heirs, predecessors, successors, and assigns. Also excluded is any Judge to whom this case is assigned as well as their judicial staff and immediate family members.

108. Plaintiff reserves the right to modify or amend the definition of the proposed Class or add subclasses before the Court determines whether certification is appropriate.

109. Numerosity. The Class Members are so numerous that joinder of all members is impracticable. Though the exact identities of Class Members are unknown at this time, based on information and belief, the Class consists of over one hundred thousand individuals whose data was compromised in the Data Breach. The identities of Class Members are ascertainable through Defendant's records, Class Members' records, publication notice, self-identification, and other means.

110. Commonality. There are questions of law and fact common to the Class which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Defendant engaged in the conduct alleged herein;

b. Whether Defendant's conduct violated the FTCA and/or HIPAA;

c. Whether and to what extent Defendant had a duty to protect the Private Information of Class Members;

d. When Defendant learned of the vulnerability within its network that led to the Data Breach;

e. Whether Defendant's response to the Data Breach was adequate;

f. Whether Defendant took reasonable steps and measures to safeguard Plaintiff's and Class Members' Private Information;

g. Whether Defendant breached its duty to Class Members to safeguard their Private Information;

h. Whether hackers obtained Class Members' Private Information via the Data Breach;

i. Whether Defendant knew or should have known that its data monitoring and supervision processes were deficient;

j. Whether Defendant was aware that its business associates', vendors', and/or suppliers' data security practices, procedures, and protocols were inadequate;

k. What damages Plaintiff and Class Members suffered as a result of Defendant's misconduct;

l. Whether Defendant's conduct was negligent;

m. Whether Defendant were unjustly enriched;

n. Whether Plaintiff and Class Members are entitled to actual and/or statutory damages;

o. Whether Plaintiff and Class Members are entitled to lifetime credit or identity monitoring and monetary relief; and

p. Whether Plaintiff and Class Members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

111. Typicality. Plaintiff's claims are typical of those of other Class Members because Plaintiff's Private Information, like that of every other Class Member, was compromised in the Data Breach. Plaintiff's claims are typical of those of the other Class Members because, *inter alia*,

all Class Members were injured through the common misconduct of Defendant. Plaintiff is advancing the same claims and legal theories on behalf of himself and all other Class Members, and there are no defenses that are unique to Plaintiff. The claims of Plaintiff and those of Class Members arise from the same operative facts and are based on the same legal theories.

112. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of Class Members. Plaintiff's counsel is competent and experienced in litigating class actions, including data privacy litigation of this kind.

113. Predominance. Defendant has engaged in a common course of conduct toward Plaintiff and Class Members in that all of Plaintiff's and Class Members' data was stored on the same computer systems and unlawfully accessed and exfiltrated in the same way and as a result of the same negligent acts and omissions committed by Defendant. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

114. Superiority. A Class action is superior to other available methods for the fair and efficient adjudication of this controversy and no unusual difficulties are likely to be encountered in the management of this class action. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a Class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, conducting this action as a class action presents far fewer management

difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

115. Defendant has acted and/or refused to act on grounds generally applicable to the Class such that final injunctive relief and/or corresponding declaratory relief is appropriate as to the Class as a whole.

116. Finally, all members of the proposed Class are readily ascertainable. Defendant has access to the names and addresses and/or email addresses of Class Members affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by Defendant.

CLAIMS FOR RELIEF

COUNT I
NEGLIGENCE
(ON BEHALF OF PLAINTIFF AND THE NATIONWIDE CLASS)

117. Plaintiff restates and realleges all of the allegations in the preceding paragraphs as if fully set forth herein.

118. Defendant knowingly collected, came into possession of, and maintained Plaintiff's and Class Members' Private Information, and had a duty to exercise reasonable care in safeguarding, securing, and protecting such Information from being disclosed, compromised, lost, stolen, and misused by unauthorized parties.

119. Defendant knew or should have known of the risks inherent in collecting the Private Information of Plaintiff and Class Members and the importance of adequate security. Defendant was on notice because, on information and belief, it knew or should have known that the Private Information would be an attractive target for cyberattacks.

120. Defendant owed a duty of care to Plaintiff and Class Members whose Private Information was entrusted to them. Defendant's duties included, but were not limited to, the following:

a. To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, supervising, monitoring, and protecting the Private Information in its possession (and in the possession of its business associates, vendors, and/or suppliers);

b. To protect Private Information entrusted to it using reasonable and adequate security procedures and systems compliant with industry standards;

c. To have procedures, including but not limited to monitoring and supervision procedures, in place to prevent the loss or unauthorized dissemination of Private Information in its possession;

d. To employ reasonable security measures and otherwise protect the Private Information of Plaintiff and Class Members pursuant to HIPAA and the FTCA;

e. To implement processes to quickly detect a data breach and to timely act on warnings about data breaches; and

f. To promptly notify Plaintiff and Class Members of the Data Breach, and to precisely disclose the type(s) of information compromised.

121. Defendant's duty to employ reasonable data security measures arose, in part, under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

122. Defendant's duty also arose because Defendant was bound by industry standards to protect Plaintiff's and Class Members' confidential Private Information.

123. Plaintiff and Class Members were foreseeable victims of any inadequate security practices on the part of Defendant and its associates, vendors, and/or suppliers, and Defendant owed Plaintiff and Class Members a duty of care to not subject them to an unreasonable risk of harm.

124. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class Members by failing to exercise reasonable care in protecting and safeguarding Plaintiff's and Class Members' Private Information within its care.

125. Defendant, by its actions and/or omissions, breached its duty of care by failing to provide, or acting with reckless disregard for, fair, reasonable, or adequate data security practices to safeguard the Private Information of Plaintiff and Class Members.

126. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;

b. Failing to adequately monitor the security of the Private Information;

c. Allowing unauthorized access to Class Members' Private Information;

d. Failing to comply with the FTCA;

e. Failing to comply with HIPAA; and

f. Failing to comply with other state laws and regulations, as further set forth herein.

127. Defendant had a special relationship with Plaintiff and Class Members. Plaintiff's and Class Members' willingness to entrust Defendant with their Private Information was predicated on the understanding that Defendant and its business associates, which business associates Defendant has an obligation to monitor and supervise, would take adequate data security precautions to protect such Information.

128. Defendant's breach of duties owed to Plaintiff and Class Members caused Plaintiff's and Class Members' Private Information to be compromised, exfiltrated, and misused, as alleged herein.

129. Defendant's breaches of duty also caused a substantial, imminent risk to Plaintiff and Class Members of identity theft, loss of control over their Private Information, and/or loss of time and money to monitor their accounts for fraud.

130. As a result of Defendant's negligence in breach of its duties owed to Plaintiff and Class Members, Plaintiff and Class Members are in danger of imminent harm in that their Private Information, which is still in the possession of third parties, will be used for fraudulent purposes.

131. Defendant also had independent duties under state laws that required them to reasonably safeguard Plaintiff's and Class Members' Private Information and promptly notify them about the Data Breach.

132. As a direct and proximate result of Defendant's negligent conduct, Plaintiff and Class Members have suffered damages as alleged herein and are at imminent risk of further harm.

133. The injury and harm that Plaintiff and Class Members suffered was reasonably foreseeable.

134. Plaintiff and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

135. In addition to monetary relief, Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, *inter alia*, strengthen its data security monitoring procedures, conduct periodic audits of those procedures, and provide lifetime credit monitoring and identity theft insurance to Plaintiff and Class Members.

COUNT II
BREACH OF IMPLIED CONTRACT
(ON BEHALF OF PLAINTIFF AND THE NATIONWIDE CLASS)

136. Plaintiff restates and realleges the allegations in the preceding paragraphs as if fully set forth herein.

137. Defendant provided insurance services to Plaintiff and Class Members through their respective employers. Plaintiff and Class Members formed an implied contract with Defendant regarding the provision of those services, including by Plaintiff and Class Members providing their Private Information to Defendant in exchange for the services offered.

138. Through Defendant's offering of services, it knew or should have known that it needed to protect Plaintiff's and Class Members' confidential Private Information in accordance with Defendant's policies, practices, and applicable state and federal law.

139. As consideration, Plaintiff and Class Members turned over valuable Private Information to Defendant. Accordingly, Plaintiff and Class Members bargained with Defendant to securely maintain and store their Private Information.

140. Defendant accepted possession of Plaintiff's and Class Members' Private Information for the purpose of providing services to Plaintiff and Class Members.

141. In delivering their Private Information to Defendant in exchange for Defendant's services, Plaintiff and Class Members intended and understood that Defendant would adequately safeguard the Private Information as part of those services.

142. Defendant's implied promises to Plaintiff and Class Members include, but are not limited to, (1) taking steps to ensure that anyone who is granted access to Private Information, including its business associates, vendors, and/or suppliers, also protect the confidentiality of that data; (2) taking steps to ensure that the Private Information that is placed in the control of its business associates, vendors, and/or suppliers is restricted and limited to achieve an authorized business purpose; (3) restricting access to qualified and trained employees, business associates, vendors, and/or suppliers; (4) designing and implementing appropriate retention policies to protect the Private Information against criminal data breaches; (5) applying or requiring proper encryption; (6) implementing multifactor authentication for access; (7) complying with HIPAA standards to make sure that Plaintiff's and Class Members' PHI would remain protected; and (8) taking other steps to protect against foreseeable data breaches.

143. Plaintiff and Class Members would not have entrusted their Private Information to Defendant in the absence of such an implied contract.

144. Had Defendant disclosed to Plaintiff and the Class that it did not have adequate data security and data supervisory practices to ensure the security of their sensitive data, Plaintiff and Class Members would not have provided their Private Information to Defendant.

145. As a provider of health insurance services, Defendant recognized (or should have recognized) that Plaintiff's and Class Member's Private Information is highly sensitive and must be protected, and that this protection was of material importance as part of the bargain with Plaintiff and the Class.

146. Defendant violated these implied contracts by failing to employ reasonable and adequate security measures to secure Plaintiff's and Class Members' Private Information.

Defendant further breached these implied contracts by failing to comply with its promise to abide by HIPAA.

147. Additionally, Defendant breached the implied contracts with Plaintiff and Class Members by failing to ensure the confidentiality and integrity of electronic protected health information they created, received, maintained, and transmitted, in violation of 45 CFR 164.306(a)(1).

148. Defendant further breached the implied contracts with Plaintiff and Class Members by failing to implement policies and procedures to prevent, detect, contain, and correct security violations, in violation of 45 CFR 164.308(a)(1).

149. Defendant further breached the implied contracts with Plaintiff and Class Members by failing to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity, in violation of 45 CFR 164.308(a)(6)(ii).

150. Defendant further breached the implied contracts with Plaintiff and Class Members by failing to protect against any reasonably anticipated threats or hazards to the security or integrity of electronic protected health information, in violation of 45 CFR 164.306(a)(2).

151. Defendant further breached the implied contracts with Plaintiff and Class Members by failing to protect against any reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information, in violation of 45 CFR 164.306(a)(3).

152. Defendant further breached the implied contracts with Plaintiff and Class Members by failing to ensure compliance with the HIPAA security standard rules by its workforce violations, in violation of 45 CFR 164.306(a)(94).

153. Defendant further breached the implied contracts with Plaintiff and Class Members by impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons, in violation of 45 CFR 164.502, *et seq*.

154. Defendant further breached the implied contracts with Plaintiff and Class Members by failing to design, implement, and enforce policies and procedures establishing physical administrative safeguards to reasonably safeguard protected health information, in violation of 45 CFR 164.530(c).

155. Defendant further breached the implied contracts with Plaintiff and Class Members by failing to ensure the confidentiality, integrity, and availability of all electronic protected health information its business associate(s) "create, receive, maintain, or transmit" and "protect against any reasonably anticipated threats or hazards to the security or integrity of such information," in violation of 45 C.F.R. § 164.306 (emphasis added).

156. Defendant further breached the implied contracts with Plaintiff and Class Members by otherwise failing to safeguard Plaintiff's and Class Members' PHI.

157. A meeting of the minds occurred, as Plaintiff and Class Members agreed, *inter alia*, to provide accurate and complete Private Information and to pay Defendant in exchange for Defendant's agreement to, *inter alia*, protect their Private Information.

158. Plaintiff and Class Members have been damaged by Defendant's conduct, including the harms and injuries arising from the Data Breach now and in the future, as alleged herein.

COUNT III
BREACH OF THIRD-PARTY BENEFICIARY CONTRACT
(ON BEHALF OF PLAINTIFF AND THE NATIONWIDE CLASS)

159. Plaintiff restates and realleges the allegations in the preceding paragraphs as if fully set forth herein.

160. This Count is pleaded in the alternative to Count II above.

161. Upon information and belief, Defendant entered into virtually identical contracts with its clients, including Lapham, to provide employee health plan services to them. These services included material terms regarding Defendant's implementation of data security practices, procedures, and protocols sufficient to safeguard the Private Information that was to be entrusted to it.

162. Such contracts were made expressly for the benefit of Plaintiff and the Class, as it was their Private Information that Defendant agreed to receive and protect through its services. Thus, the benefit of collection and protection of the Private Information belonging to Plaintiff and the Class was the direct and primary objective of the contracting parties and Plaintiff and Class Members were direct and express beneficiaries of such contracts.

163. Defendant knew that if it were to breach these contracts with its clients, Plaintiff and the Class, would be harmed.

164. Defendant breached its contracts with its clients and, as a result, Plaintiff and Class Members were affected by this Data Breach when Defendant failed to use reasonable data security and/or business associate monitoring measures that could have prevented the Data Breach.

165. As foreseen, Plaintiff and the Class were harmed by Defendant's failure to use reasonable data security measures to securely store and protect the files in its care, including but not limited to, the continuous and substantial risk of harm through the loss of their Private Information.

166. Accordingly, Plaintiff and the Class are entitled to damages in an amount to be determined at trial, along with costs and attorneys' fees incurred in this action.

COUNT IV
UNJUST ENRICHMENT/QUASI CONTRACT
(ON BEHALF OF PLAINTIFF AND THE NATIONWIDE CLASS)

167. Plaintiff restates and realleges the allegations in the preceding paragraphs as if fully set forth herein.

168. This Count is pleaded in the alternative to Counts II and III above.

169. Plaintiff and Class Members conferred a benefit on Defendant. Specifically, they provided Defendant with their Private Information, which Private Information has inherent value. In exchange, Plaintiff and Class Members should have been entitled to Defendant's adequate protection and supervision of their Private Information, especially in light of their special relationship.

170. Defendant knew that Plaintiff and Class Members conferred a benefit upon it and has accepted and retained that benefit by accepting and retaining the Private Information entrusted to it. Defendant profited from Plaintiff's retained data and used Plaintiff's and Class Members' Private Information for business purposes.

171. Defendant failed to secure Plaintiff's and Class Members' Private Information and, therefore, did not fully compensate Plaintiff or Class Members for the value that their Private Information provided.

172. Defendant acquired the Private Information through inequitable record retention as it failed to disclose the inadequate data security practices previously alleged.

173. If Plaintiff and Class Members had known that Defendant would not use adequate data security practices, procedures, and protocols to adequately monitor, supervise, and secure

their Private Information, they would have required that alternative choices be made by their respective employers that excluded Defendant.

174. Plaintiff and Class Members have no adequate remedy at law.

175. Under the circumstances, it would be unjust for Defendant to be permitted to retain any of the benefits that Plaintiff and Class Members conferred upon it.

176. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) the imminent and substantial risk of actual identity theft; (ii) the loss of the opportunity to control how their Private Information is used; (iii) the compromise, publication, and/or theft of their Private Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private Information; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Private Information in its continued possession; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

177. Plaintiff and Class Members are entitled to full refunds, restitution, and/or damages from Defendant and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by Defendant from its wrongful conduct. This can be accomplished by

establishing a constructive trust from which the Plaintiff and Class Members may seek restitution or compensation.

178. Plaintiff and Class Members may not have an adequate remedy at law against Defendant, and accordingly, they plead this claim for unjust enrichment in addition to, or in the alternative to, other claims pleaded herein.

COUNT V
BREACH OF CONFIDENCE
(ON BEHALF OF PLAINTIFF AND THE NATIONWIDE CLASS)

179. Plaintiff restates and realleges the allegations in the preceding paragraphs as if fully set forth herein.

180. Plaintiff and Class Members have an interest, both equitable and legal, in the Private Information about them that was conveyed to, collected by, and maintained by Defendant and ultimately accessed and acquired in the Data Breach.

181. As a provider of employer health plans, Defendant has a special relationship with the employees of its clients, including Plaintiff and Class Members. Because of that special relationship, Defendant was provided with and stored Plaintiff's and Class Members' Private Information and had a duty to ensure that such was maintained in confidence.

182. Individuals like Plaintiff and Class Members have a privacy interest in personal, medical and other matters, and Defendant had a duty not to permit the disclosure of such matters concerning Plaintiff and Class Members.

183. As a result of the parties' special relationship, Defendant had possession and knowledge of highly sensitive and confidential PHI and PII belonging to Plaintiff and Class Members, information that was not generally known.

184. Plaintiff and Class Members did not consent nor authorize Defendant to release or disclose their Private Information to an unknown criminal actor.

185. Defendant breached its duty of confidence owed to Plaintiff and Class Members by, among other things: (a) failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of employee member information that resulted in the unauthorized access and compromise of Plaintiff's and Class Members' Private Information; (b) mishandling its data security by failing to assess the sufficiency of its safeguards (and those of its business associates, vendors, and/or suppliers) in place to control these risks; (c) failing to evaluate and adjust its information security program in light of the circumstances alleged herein; (d) failing to follow its own privacy policies and practices published to clients and their employees; and (e) making an unauthorized and unjustified disclosure and release of Plaintiff's and Class Members' Private Information to a criminal third party.

186. But for Defendant's wrongful breach of its duty of confidence owed to Plaintiff and Class Members, their Private Information would not have been compromised.

187. As a direct and proximate result of Defendant's wrongful breach of its duty of confidence, Plaintiff and Class Members have suffered and will continue to suffer the injuries alleged herein.

188. It would be inequitable for Defendant to retain the benefit of controlling and maintaining Plaintiff's and Class Members' Private Information at the expense of Plaintiff and Class Members.

189. Plaintiff and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, and/or disgorgement or restitution, in an amount to be proven at trial.

COUNT VI
INJUNCTIVE/DECLARATORY RELIEF
(ON BEHALF OF PLAINTIFF AND THE NATIONWIDE CLASS)

190. Plaintiff restates and realleges the allegations in the preceding paragraphs as if fully set forth herein.

191. Under the Declaratory Judgment Act, 28 U.S.C. § 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and to grant further necessary relief. Furthermore, the Court has broad authority to restrain acts that are tortious and violate the terms of the federal and state statutes described in this Complaint.

192. Defendant owes a duty of care to Plaintiff and Class Members, which required them to adequately monitor and safeguard Plaintiff's and Class Members' Private Information.

193. Defendant and its associates, vendors, and/or suppliers still possess the Private Information belonging to Plaintiff and Class Members.

194. Plaintiff alleges that Defendant's data security measures remain inadequate. Furthermore, Plaintiff continues to suffer injury as a result of the compromise of his Private Information and the risk remains that further compromises of his Private Information will occur in the future.

195. Under its authority pursuant to the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendant owes a legal duty to secure its clients' employees' Private Information under the common law, HIPAA, and the FTCA;

b. Defendant's existing data monitoring measures do not comply with its explicit or implicit contractual obligations and duties of care to provide reasonable data

security procedures and practices that are appropriate to protect Private Information; and

c. Defendant continues to breach this legal duty by failing to employ reasonable measures to secure its clients' employees' Private Information.

196. This Court should also issue corresponding prospective injunctive relief requiring Defendant to employ adequate security protocols consistent with legal and industry standards to protect the highly sensitive Private Information that remains in its possession and control, including the following:

a. Order Defendant to provide lifetime credit monitoring and identity theft insurance to Plaintiff and Class Members.

b. Order that, to comply with Defendant's explicit or implicit contractual obligations and duties of care, Defendant must implement and maintain reasonable security and monitoring measures, including, but not limited to:

i. engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

ii. engaging third-party security auditors and internal personnel to run automated security monitoring;

iii. auditing, testing, and training its security personnel regarding any new or modified procedures;

iv. segmenting its user applications by, among other things, creating firewalls and access controls so that if one area is compromised, hackers cannot gain access to other portions of Defendant's systems;

v. conducting regular database scanning and security checks;

vi. routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

vii. meaningfully educating its clients and its clients' employees about the threats they face with regard to the security of their Private Information, as well as the steps that should be taken to protect themselves.

197. If an injunction is not issued, Plaintiff will suffer irreparable injury and will lack an adequate legal remedy to prevent another data breach at Defendant. The risk of another such breach is real, immediate, and substantial. If another breach at Defendant occurs, Plaintiff will not have an adequate remedy at law because many of the resulting injuries are not readily quantifiable.

198. The hardship to Plaintiff if an injunction does not issue exceeds the hardship to Defendant if an injunction is issued. Plaintiff will likely be subjected to substantial, continued identity theft and other related damages if an injunction is not issued. On the other hand, the cost of Defendant's compliance with an injunction requiring reasonable prospective data security measures is relatively minimal, and Defendant has a pre-existing legal obligation to employ such measures.

199. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing a subsequent data breach at

Defendant, thus preventing future injury to Plaintiff and other individuals whose Private Information would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and the Class described above, seeks the following relief:

a. An order certifying this action as a Class action under Fed. R. Civ. P. 23, defining the Class as requested herein, appointing the undersigned as Class counsel, and finding that Plaintiff is a proper representative of the Class requested herein;

b. Judgment in favor of Plaintiff and Class Members awarding them appropriate monetary relief, including actual damages, statutory damages, equitable relief, restitution, disgorgement, and statutory costs;

c. An order providing injunctive and other equitable relief as necessary to protect the interests of the Class as requested herein;

d. An order instructing Defendant to purchase or provide funds for lifetime credit monitoring and identity theft insurance to Plaintiff and Class Members;

e. An order requiring Defendant to pay the costs involved in notifying Class Members about the judgment and administering the claims process;

f. A judgment in favor of Plaintiff and Class Members awarding them prejudgment and post-judgment interest, reasonable attorneys' fees, costs, and expenses as allowable by law; and

g. An award of such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury on all triable issues.

DATED: July 7, 2023

Respectfully submitted,

/s/ Nicholas Sandercock

Nicholas Sandercock
Mason A. Barney (*pro hac vice* to be filed)
Tyler J. Bean (*pro hac vice* to be filed)
SIRI & GLIMSTAD LLP
745 Fifth Avenue, Suite 500
New York, New York 10151
Tel: (212) 532-1091
E: nsandercock@sirillp.com
E: mbarney@sirillp.com
E: tbean@sirillp.com

Attorneys for Plaintiff